



Welcome United States Patent and Trademark Office

☐ Search Results

BROWSE

SEARCH

IEEE XPLORE GUIDE

Results for "( ( microprocessor&lt;in&gt;metadata ) &lt;and&gt; ( cryptography&lt;in&gt;metadata ) )"

☒ e-mail
Your search matched **153** of **1566306** documents.A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

## » Search Options

[View Session History](#)
[New Search](#)

## Modify Search


☐ Check to search only within this results set
Display Format: ☒ Citation ☐ Citation & Abstract

## » Key

IEEE JNL IEEE Journal or Magazine

IET JNL IET Journal or Magazine

IEEE CNF IEEE Conference Proceeding

IET CNF IET Conference Proceeding

IEEE STD IEEE Standard

[Select All](#) [Deselect All](#)

View: 1-25 | 26-5

- ☐ 1. **Architectural extensions for elliptic curve cryptography over GF(2<sup>m</sup>) microprocessors**  
 Eberle, H.; Wander, A.; Gura, N.; Sheueling Chang-Shantz; Gupta, V.;  
[Application-Specific Systems, Architecture Processors, 2005. ASAP 2005. 16th International Conference on](#)  
 23-25 July 2005 Page(s):343 - 349  
 Digital Object Identifier 10.1109/ASAP.2005.15  
[AbstractPlus](#) | Full Text: [PDF](#)(312 KB) IEEE CNF  
[Rights and Permissions](#)
- ☐ 2. **Design and implementation of a private and public key crypto processor application to a security system**  
 Ho Won Kim; Sunggu Lee;  
[Consumer Electronics, IEEE Transactions on](#)  
 Volume 50, Issue 1, Feb 2004 Page(s):214 - 224  
 Digital Object Identifier 10.1109/TCE.2004.1277865  
[AbstractPlus](#) | Full Text: [PDF](#)(1093 KB) IEEE JNL  
[Rights and Permissions](#)
- ☐ 3. **Application-specific customisation of multi-threaded soft processors**  
 Dimond, R.; Mencer, O.; Luk, W.;  
[Computers and Digital Techniques, IEE Proceedings-](#)  
 Volume 153, Issue 3, 2 May 2006 Page(s):173 - 180  
 Digital Object Identifier 10.1049/ip-cdt:20050177  
[AbstractPlus](#) | Full Text: [PDF](#)(344 KB) IET JNL
- ☐ 4. **High-speed implementation of an ECC-based wireless authentication processor microprocessor**  
 Aydos, M.; Yanik, T.; Koc, C.K.;  
[Communications, IEE Proceedings-](#)  
 Volume 148, Issue 5, Oct. 2001 Page(s):273 - 279  
 Digital Object Identifier 10.1049/ip-com:20010511  
[AbstractPlus](#) | Full Text: [PDF](#)(670 KB) IET JNL
- ☐ 5. **A high-speed ECC-based wireless authentication on an ARM microprocessor**  
 Aydos, M.; Yanik, T.; Koc, C.K.;  
[Computer Security Applications, 2000. ACSAC '00. 16th Annual Conference](#)  
 11-15 Dec. 2000 Page(s):401 - 409

Digital Object Identifier 10.1109/ACSAC.2000.898895

[AbstractPlus](#) | Full Text: [PDF\(588 KB\)](#) IEEE CNF  
[Rights and Permissions](#)

- ☐ **6. An area-efficient universal cryptography processor for smart cards**  
Eslami, Y.; Sheikholeslami, A.; Gulak, P.G.; Masui, S.; Mukaida, K.;  
[Very Large Scale Integration \(VLSI\) Systems, IEEE Transactions on](#)  
Volume 14, Issue 1, Jan. 2006 Page(s):43 - 56  
Digital Object Identifier 10.1109/TVLSI.2005.863188  
[AbstractPlus](#) | Full Text: [PDF\(976 KB\)](#) IEEE JNL  
[Rights and Permissions](#)
  
- ☐ **7. Cryptographic smart cards**  
Naccache, D.; M'Raihi, D.;  
[Micro, IEEE](#)  
Volume 16, Issue 3, June 1996 Page(s):14, 16 - 24  
Digital Object Identifier 10.1109/40.502402  
[AbstractPlus](#) | [References](#) | Full Text: [PDF\(1752 KB\)](#) IEEE JNL  
[Rights and Permissions](#)
  
- ☐ **8. IT security project: implementation of the Advanced Encryption Standard smart card**  
Schramm, K.; Paar, C.;  
[Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004 Conference on](#)  
Volume 1, 2004 Page(s):176 - 180 Vol.1  
Digital Object Identifier 10.1109/ITCC.2004.1286446  
[AbstractPlus](#) | Full Text: [PDF\(1370 KB\)](#) IEEE CNF  
[Rights and Permissions](#)
  
- ☐ **9. The Montgomery modular inverse-revisited**  
Savas, E.; Koc, C.K.;  
[Computers, IEEE Transactions on](#)  
Volume 49, Issue 7, July 2000 Page(s):763 - 766  
Digital Object Identifier 10.1109/12.863048  
[AbstractPlus](#) | [References](#) | Full Text: [PDF\(132 KB\)](#) IEEE JNL  
[Rights and Permissions](#)
  
- ☐ **10. WLAN security processor**  
Smyth, N.; McLoone, M.; McCanny, J.V.;  
[Circuits and Systems I: Regular Papers, IEEE Transactions on \[see also Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on\]](#)  
Volume 53, Issue 7, July 2006 Page(s):1506 - 1520  
Digital Object Identifier 10.1109/TCSI.2006.877888  
[AbstractPlus](#) | Full Text: [PDF\(768 KB\)](#) IEEE JNL  
[Rights and Permissions](#)
  
- ☐ **11. Programmable active memories: reconfigurable systems come of age**  
Vuillemin, J.E.; Bertin, P.; Roncin, D.; Shand, M.; Touati, H.H.; Boucard, P.;  
[Very Large Scale Integration \(VLSI\) Systems, IEEE Transactions on](#)  
Volume 4, Issue 1, March 1996 Page(s):56 - 69  
Digital Object Identifier 10.1109/92.486081  
[AbstractPlus](#) | [References](#) | Full Text: [PDF\(1588 KB\)](#) IEEE JNL  
[Rights and Permissions](#)
  
- ☐ **12. Efficient Implementation of Galois Field Fixed Field Constant Multiplication**  
Elbirt, A.; Paar, C.;  
[Information Technology: New Generations, 2006. ITNG 2006. Third International Conference on](#)  
10-12 April 2006 Page(s):172 - 177

Digital Object Identifier 10.1109/ITNG.2006.59

[AbstractPlus](#) | Full Text: [PDF\(216 KB\)](#) IEEE CNF  
[Rights and Permissions](#)

- ☐ **13. Representation of the large numbers with accounting of microprocessor**  
Igumnov, V.S.;  
[Electron Devices and Materials, 2005. Proceedings. 6th Annual. 2005 Internat Workshop and Tutorials on](#)  
1-5 July 2005 Page(s):233 - 235  
[AbstractPlus](#) | Full Text: [PDF\(129 KB\)](#) IEEE CNF  
[Rights and Permissions](#)
  
- ☐ **14. Secure scan: a design-for-test architecture for crypto chips**  
Bo Yang; Kaijie Wu; Karri, R.;  
[Design Automation Conference, 2005. Proceedings. 42nd](#)  
13-17 June 2005 Page(s):135 - 140  
[AbstractPlus](#) | Full Text: [PDF\(354 KB\)](#) IEEE CNF  
[Rights and Permissions](#)
  
- ☐ **15. Accelerating private-key cryptography via multithreading on symmetric r**  
Dongara, P.; Vijaykumar, T.N.;  
[Performance Analysis of Systems and Software, 2003. ISPASS. 2003 IEEE In Symposium on](#)  
6-8 March 2003 Page(s):58 - 69  
[AbstractPlus](#) | Full Text: [PDF\(869 KB\)](#) IEEE CNF  
[Rights and Permissions](#)
  
- ☐ **16. Design of integrated circuits fully testable for delay-faults and multifaults**  
Devadas, S.; Keutzer, K.;  
[Test Conference, 1990. Proceedings., International](#)  
10-14 Sept. 1990 Page(s):284 - 293  
Digital Object Identifier 10.1109/TEST.1990.114034  
[AbstractPlus](#) | Full Text: [PDF\(916 KB\)](#) IEEE CNF  
[Rights and Permissions](#)
  
- ☐ **17. Low complexity implementation of modified McEliece algorithms**  
Honary, B.; Edgar, J.;  
[Security and Cryptography Applications to Radio Systems, IEE Colloquium on](#)  
1994 Page(s):12/1 - 12/2  
[AbstractPlus](#) | Full Text: [PDF\(120 KB\)](#) IET CNF
  
- ☐ **18. IEEE Standard Specifications for Public-Key Cryptography**  
29 Aug. 2000  
[AbstractPlus](#) | Full Text: [PDF\(1364 KB\)](#) IEEE STD
  
- ☐ **19. Area-throughput trade-offs for fully pipelined 30 to 70 Gbits/s AES proce:**  
Hodjat, A.; Verbaauwhede, I.;  
[Computers, IEEE Transactions on](#)  
Volume 55, Issue 4, April 2006 Page(s):366 - 372  
Digital Object Identifier 10.1109/TC.2006.49  
[AbstractPlus](#) | Full Text: [PDF\(1912 KB\)](#) IEEE JNL  
[Rights and Permissions](#)
  
- ☐ **20. Cipher instruction search attack on the bus-encryption security microcoi**  
**DS5002FP**  
Kuhn, M.G.;  
[Computers, IEEE Transactions on](#)  
Volume 47, Issue 10, Oct. 1998 Page(s):1153 - 1157

Digital Object Identifier 10.1109/12.729797

[AbstractPlus](#) | [References](#) | Full Text: [PDF\(96 KB\)](#) IEEE JNL  
[Rights and Permissions](#)

- ☐ **21. Special-Purpose Hardware in Cryptanalysis: The Case of 1,024-Bit RSA**  
Willi Geiselmann; Rainer Steinwandt;  
[Security & Privacy Magazine, IEEE](#)  
Volume 5, Issue 1, Jan.-Feb. 2007 Page(s):63 - 66  
Digital Object Identifier 10.1109/MSP.2007.20  
[AbstractPlus](#) | Full Text: [PDF\(724 KB\)](#) IEEE JNL  
[Rights and Permissions](#)
- ☐ **22. Cryptographic Processors-a survey**  
Anderson, R.; Bond, M.; Clulow, J.; Skorobogatov, S.;  
[Proceedings of the IEEE](#)  
Volume 94, Issue 2, Feb. 2006 Page(s):357 - 369  
Digital Object Identifier 10.1109/JPROC.2005.862423  
[AbstractPlus](#) | Full Text: [PDF\(472 KB\)](#) IEEE JNL  
[Rights and Permissions](#)
- ☐ **23. Design of flexible GF(2/sup m/) elliptic curve cryptography processors**  
Benaissa, M.; Wei Ming Lim;  
[Very Large Scale Integration \(VLSI\) Systems, IEEE Transactions on](#)  
Volume 14, Issue 6, June 2006 Page(s):659 - 662  
Digital Object Identifier 10.1109/TVLSI.2006.878235  
[AbstractPlus](#) | Full Text: [PDF\(456 KB\)](#) IEEE JNL  
[Rights and Permissions](#)
- ☐ **24. Memory-free low-cost designs of advanced encryption standard using cc subexpression elimination for subfunctions in transformations**  
Shen-Fu Hsiao; Ming-Chih Chen; Chia-Shin Tu;  
[Circuits and Systems I: Regular Papers, IEEE Transactions on \[see also Circu Fundamental Theory and Applications, IEEE Transactions on\]](#)  
Volume 53, Issue 3, March 2006 Page(s):615 - 626  
Digital Object Identifier 10.1109/TCSI.2005.859052  
[AbstractPlus](#) | Full Text: [PDF\(584 KB\)](#) IEEE JNL  
[Rights and Permissions](#)
- ☐ **25. Security and performance optimization of a new DES data encryption chi**  
Verbauwhede, I.; Hoornaert, F.; Vandewalle, J.; De Man, H.J.;  
[Solid-State Circuits, IEEE Journal of](#)  
Volume 23, Issue 3, June 1988 Page(s):647 - 656  
Digital Object Identifier 10.1109/4.302  
[AbstractPlus](#) | Full Text: [PDF\(960 KB\)](#) IEEE JNL  
[Rights and Permissions](#)

View: 1-25 | [26-5](#)

Indexed by  
 Inspec<sup>®</sup>

[Help](#) [Contact Us](#) [Privacy &](#)  
© Copyright 2006 IEEE –